WITT'S PROOF THAT EVERY FINITE DIVISION RING IS A FIELD

K. N. RAGHAVAN

We present, following the exposition in Chapter 6 of the 4th edition of PROOFS FROM THE BOOK by *Martin Aigner* and *Günter Ziegler*, the proof, due to Witt from the year 1931, of the following famous theorem, due to Wedderburn from the year 1905:

$$\boxed{\textit{Every finite division ring is a field.}} \tag{1}$$

The proof proper appears finally in §5 after preparations in the earlier sections. It may be summarized as follows:

> Following Weddernburn's original method of proof, we first write down the class equation of the multiplicative group $D^\times$ of non-zero elements of a finite division ring D (see §3). Suppose that the centre $\mathfrak{z}(D)$ of D, which is evidently a finite field, is of cardinality q. Counting vector space dimensions over $\mathfrak{z}(D)$ of certain subrings of D containing $\mathfrak{z}(D)$ allows us to determine the form of the component numbers in this class equation (see (9)). Then, assuming that the dimension n of D over $\mathfrak{z}(D)$ is bigger than one, we arrive at a contradiction. For this, we check, following Witt, divisibility of the component numbers by a special integer, namely the value at q of the n^{th} cyclotomic polynomial.

1. GROUP ACTIONS

We say that a group G acts on a set X if there exists a map $G \times X \to X$, given by $(g, x) \mapsto gx$ satisfying the following axioms: $g(hx) = (gh)x$ for g, h in G and x in X; and $1x = x$ for x in X (where 1 denotes the identity element of G).

Let X and Y be sets on both of which a group G acts. A map $\phi : X \to Y$ is said to *commute with the action of* G, or simply be a *G-map*, if $\phi(gx) = g(\phi(x))$ for all x in X and g in G.

1.1. **Examples of group actions.**

Groups almost always naturally arise along with actions on sets (or other mathematical structures). For instance, the symmetric group S_n naturally acts on the set $\{1, \ldots, n\}$, it being defined as the set of bijections from this set to itself.

This write-up supplements lectures given in December 2016 at a workshop sponsored by NBHM and IMSc at SARADA COLLEGE FOR WOMEN in Salem. Comments are solicited and may please be emailed to knr.imsc@gmail.com or knr@imsc.res.in. Up-to-date version of this write-up is permanently available at http://www.imsc.res.in/∼knr/past/salem1612.pdf.

1.1.1. Left regular and conjugacy actions. Here are two actions of a group G on itself:

- $G \times G \to G$ given by $(g, x) \mapsto gx$ (where gx denotes the usual group product); this is called the *left regular action*.
- $G \times G \to G$ given by $(g, x) \mapsto gxg^{-1}$, called the *conjugacy action*.

1.1.2. Action on the left coset space. Let G/H denote the set of left cosets of a subgroup H in a group G. There is a natural action of G on G/H, given by $(g, xH) \mapsto gxH$.

1.1.3. Restriction of an action. If a group G acts on a set X and H is a subgroup of G, then the restriction to $H \times X$ of the action map $G \times X \to X$ evidently defines an action of H on X. This is called the *restriction* to H of the action of G on X.

1.2. **Orbits.** Let a group G act on a set X. We define an equivalence relation on X by: $x \sim y$ for x, y in X if there exists g in G such that $gx = y$. The resulting equivalence classes are called *orbits*. Being equivalence classes, the orbits form a partition of X.

The action of G on X is said to be *transitive* if the whole of X is a single orbit. We will presently derive a structure theorem for transitive actions (see §1.4).

The action of S_n on $\{1, \ldots, n\}$, the left regular action of G on itself, and the action of G on left cosets are all transitive. In contrast, the conjugacy action is not transitive (except when $G = \{1\}$ is the trivial group). The orbits for the conjugacy action are called the *conjugacy classes*.

1.3. **Lagrange's theorem.** Consider the restriction to a subgropup H of the left regular action of a finite group G on itself. The orbits for this action are the right cosets of H. Thus, each orbit has exactly $|H|$ elements, and there are $|H\backslash G|$ orbits—recall that $H\backslash G$ denotes the set of right cosets of H. Since the orbits form a partition of G, we conclude that $|H| \cdot |H\backslash G| = |G|$. In other words:

$$\boxed{|H| \text{ divides } |G| \text{ and the number } |H\backslash G| \text{ of right cosets of } H \text{ equals } |G|/|H|} \qquad (2)$$

The group G is also partitioned by the left cosets of H. Since each left coset has H elements, we conclude:

$$\boxed{|H| \cdot |G/H| = |G| \quad \text{and so } |G/H| = |G|/|H|} \qquad (3)$$

1.4. **The structure of an orbit.** Let a group G act transitively on a set X. Fix x in X. Let $G_x := \{g \in G \,|\, gx = x\}$ be the *stabilizer* in G of x. This is a subgroup. It is readily verified that $gG_x \mapsto gx$ defines a bijective G-map from $G/G_x \to X$.

We thus conclude, in case $|G|$ is finite, the following:

$$\boxed{X = |G/G_x| = |G|/|G_x|; \quad \text{in particular, } |X| \text{ is finite and divides } |G|} \qquad (4)$$

2. Conjugacy classes and the class equation

Let G be a group. Recall from §1.2 that conjugacy classes of G are the orbits for the conjugacy action of G on itself. Are there singleton conjugacy classes? Surely the identity element is in a class by itself. We observe:

$$\boxed{\textit{An element of } G \textit{ forms a conjugacy class by itself iff it belongs to the centre.}} \tag{5}$$

2.1. **The class equation.** Now suppose that G is finite. Summing the cardinalities of each of the conjugacy classes gives $|G|$. In view of (5), this leads to the *class equation*:

$$\boxed{|G| = |\text{centre of } G| + |C_1| + \cdots + |C_k|} \tag{6}$$

where $C_1, \ldots, C_k$ are the non-singleton conjugacy classes of G.

2.2. **An application to p-groups.** Let G be a finite group. Recall from (4) that the cardinality of every G-orbit, and therefore of every conjugacy class in G, divides $|G|$. This fact can be combined with the class equation to good effect. For instance, using them we now prove:

$$\boxed{\textit{The centre of a } p\textit{-group is non-trivial.}} \tag{7}$$

Recall that a p-group is one whose cardinality is a power of the a prime p. Let G be a p-group. Consider its class equation (6). Since $|C_i| > 1$ by definition, it follows from (4) that it is divisible by p. Reading the class equation modulo p, we see that all terms other than $|\text{centre of } G|$ are divisible by p. Thus so is $|\text{centre of } G|$, and (7) is proved.

3. The class equation for units in a finite division ring

Let D be a finite division ring. By convention, $D \neq 0$.

3.1. **The canonical homomorphism from $\mathbb{Z}$ to a ring with identity.** For a ring R with identity, there is a unique ring homomorphism—call it χ_R—from the ring $\mathbb{Z}$ of integers to R that respects the identity (i.e., such that $\chi_R(1) = 1_R$). The image of χ_R is a subring of R and lies in the centre of R. The kernel of χ_R is an ideal in $\mathbb{Z}$ and so equals $j\mathbb{Z}$ for some unique integer $j \geq 0$. Note that χ_R induces an isomorphism of $\mathbb{Z}/\text{kernel}(\chi_R)$ onto the image of χ_R: $\mathbb{Z}/j\mathbb{Z} \simeq \text{Image}(\chi_R) \subseteq R$. Note also that $j = 1$ if and only if $R = 0$.

3.2. **The canonical homomorphism from $\mathbb{Z}$ to D.** Let us now consider the kernel $j\mathbb{Z}$ (with j an integer ≥ 0) of χ_D. Since D is finite, it follows that $n \neq 0$; since $D \neq 0$, it follows that $j \neq 1$; since $\mathbb{Z}/j\mathbb{Z} \simeq \text{Image}(\chi_D)$ and the image of χ_D is an integral domain (being a subring of D), it follows that j must be a prime. We henceforth write p in place of j to emphasize this fact.

As observed in §3.1, we have the following inclusions:

$$\mathbb{Z}/p\mathbb{Z} \simeq \text{Image}(\chi_D) \subseteq \mathfrak{z}(D) \subseteq D \tag{8}$$

where $\mathfrak{z}(D)$ denotes the centre of D. Being the centre of a division ring, $\mathfrak{z}(D)$ is a field: if $x \neq 0$ in D commutes with all elements of D, then so does x^{-1}. Being a subset of D, the centre $\mathfrak{z}(D)$ is finite.

3.3. **Centralizers of elements of D.** For an element d of D denote by $\mathfrak{z}(d)$ the centralizer $\{x \in D \mid xd = dx\}$ of d. This is a subring of D containing the centre $\mathfrak{z}(D)$.

3.4. **Cardinalities of $\mathfrak{z}(D)$, D, and $\mathfrak{z}(d)$.** Any ring containing a field may be considered as a vector space over that field. By (8), we may consider $\mathfrak{z}(D)$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$. Being a finite set, $\mathfrak{z}(D)$ is of finite dimension over $\mathbb{Z}/p\mathbb{Z}$, and thus $|\mathfrak{z}(D)|$ is a power of the prime p. Henceforth, we write q for $|\mathfrak{z}(D)|$.

By (8) again, we may consider D as a vector space over $\mathfrak{z}(D)$. Being a finite set, D has finite dimension over $\mathfrak{z}(D)$, say n. Thus $|D| = q^n$.

From §3.3, we see that $\mathfrak{z}(d)$ is a vector space over $\mathfrak{z}(D)$. Being a finite set, $\mathfrak{z}(d)$ has finite dimension over $\mathfrak{z}(D)$, say $k(d)$. Thus $|\mathfrak{z}(d)| = q^{k(d)}$.

3.5. **The class equation for $D^\times$.** The set $D^\times$ of non-zero elements of D forms a finite group under multiplication. We write the class equation for $D^\times$.

We have $|D^\times| = |D| - 1 = q^n - 1$. The centre of $D^\times$ is just $\mathfrak{z}(D) \setminus \{0\}$ and so its cardinality is $|\mathfrak{z}(D)| - 1 = q - 1$.

Now suppose d belongs to a non-singleton conjugacy class of $D^\times$. Then by (4), the cardinality of that class equals $|D^\times|/|\mathfrak{z}^\times(d)|$ where $\mathfrak{z}^\times(d)$ denotes the centralizer $\{c \in D^\times \mid cd = dc\}$ in $D^\times$ of d. But $\mathfrak{z}^\times(d) = \mathfrak{z}(d) \setminus \{0\}$, and so $|\mathfrak{z}^\times(d)| = |\mathfrak{z}(d)| - 1 = q^{k(d)} - 1$, where $k(d)$ denotes the dimension of $\mathfrak{z}(d)$ as a vector space over $\mathfrak{z}(D)$. We conclude that the conjugacy class of d has cardinality $(q^n - 1)/(q^{k(d)} - 1)$. Note that $k(d) < n$ since the class is not a singleton by assumption.

Now choose representatives $d_1, \ldots, d_\ell$ for all non-singleton conjugacy classes in $D^\times$. Denote by $k_1, \ldots, k_\ell$ the dimensions over $\mathfrak{z}(D)$ of the centralizers $\mathfrak{z}(d_1), \ldots, \mathfrak{z}(d_\ell)$. The class equation for $D^\times$ now reads as follows:

$$\boxed{q^n - 1 = (q-1) + \frac{q^n - 1}{q^{k_1} - 1} + \cdots + \frac{q^n - 1}{q^{k_\ell} - 1}} \tag{9}$$

We now observe that k_i divides n for each i, $1 \leq i \leq \ell$. This follows by invoking the following with q in place of s, and n in place of m, and k_i in place of k:

> *Let $s \geq 2$ be an integer. Let $1 \leq k \leq m$ be integers.*
> *Then $s^k - 1$ divides $s^m - 1$ if and only if k divides m.*

For a proof of this claim, let a and r be integers such that $m = ak + r$ and $0 \leq r < k$. The polynomial $x^m - 1$ can be written

$$x^m - 1 = (x^k - 1)(x^{(a-1)k+r} + x^{(a-2)k+r} + \cdots + x^{k+r} + x^r) + (x^r - 1) \tag{10}$$

In particular, $s^m - 1 \equiv s^r - 1 \pmod{s^k - 1}$. Since $s \geq 2$, we have $0 \leq s^r - 1 < s^k - 1$, so that $s^r - 1$ is the remainder when $s^m - 1$ is divided by $s^k - 1$. Thus $s^k - 1$ divides $s^m - 1$ if and only if $s^r - 1 = 0$ or $r = 0$, which holds if and only if k divides m.

4. Euler totient function and cyclotomic polynomials

Let n be a positive integer. Put $[n] := \{1, \ldots, n\}$. For d a factor of n, put

$$[n]_d := \{k \in [n] \,|\, (k, n) = d\} \tag{11}$$

where (k, n) denotes the g.c.d. of k and n. Evidently, for each k in $[n]$, the g.c.d. (k, n) equals d for some factor of n (including 1 and n). Thus we have a partition of $[n]$ as follows into disjoint subsets:

$$[n] = \bigsqcup_{d|n} [n]_d \tag{12}$$

4.1. **Euler totient function.** The function $n \mapsto |[n]_1|$ on positive integers is called the *Euler totient function* and denoted by ϕ. In other words, $\phi(n)$ is by definition the number of positive integers that are at most n and coprime to n.

Let d and n be positive integers such that $d|n$. Multiplication by d sets up a bijection between $[n]_d$ and $[n/d]_1$:

$$[n/d]_1 \simeq [n]_d \quad \text{by } k \mapsto dk \tag{13}$$

By taking cardinalities of both sides of (12), we obtain, in view of (13):

$$\boxed{n = \sum_{e|n} \phi(e)} \tag{14}$$

4.2. **n^{th} roots of unity.** A complex number z is called an n^{th} *root of unity* if $z^n = 1$, or, equivalently if z is a root of the equation $x^n - 1 = 0$. Being of degree n, the polynomial $x^n - 1$ can have at most n distinct complex roots. On the other hand, $e^{2\pi ik/n}$, k in $[n]$, are n distinct n^{th} roots of unity. Thus these are all the n^{th} roots of unity and we have:

$$\boxed{x^n - 1 = \prod_{k \in [n]} (x - e^{2\pi ik/n})} \tag{15}$$

4.3. **Primitive n^{th} roots of unity.** For k in $[n]$ such that $(k, n) = 1$, the n^{th} root of unity $e^{2\pi ik/n}$ is *primitive*, i.e., it is not an m^{th} root of unity for any integer m less than n: indeed, $(e^{2\pi ik/n})^m = 1$ only if km/n is an integer, which in turn is only if m is a multiple of n (since $(k, n) = 1$ by assumption).

For k in $[n]$ put $d = (k, n)$. Then k/d and n/d are coprime integers and $e^{2\pi ik/n} = e^{2\pi i \frac{k/d}{n/d}}$ is a primitive d^{th} root of unity.

Thus $e^{2\pi ik/n}$, k in $[n]_1$, are all the primitive n^{th} roots of unity.

4.4. **Cyclotomic polynomials.** We define the n^{th} cyclotomic polynomial to be:

$$\boxed{\Phi_n(x) := \prod_{k \in [n],\ (k,n)=1} (x - e^{2\pi ik/n})} \tag{16}$$

Evidently every d^{th} root of unity for $d|n$ is an n^{th} root of unity. And, as observed in §4.3, every n^{th} root of unity is a primitive d^{th} root of unity for a unique factor d of n. Thus

$$x^n - 1 = \prod_{d|n} \prod_{k \in [n]_d} (x - e^{2\pi i \frac{k/d}{n/d}}) = \prod_{d|n} \Phi_{n/d}(x) \quad \text{and so} \quad \boxed{x^n - 1 = \prod_{e|n} \Phi_e(x)} \tag{17}$$

We may rewrite (17) as follows:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{e|n,\ e \neq n} \Phi_e(x)} \tag{18}$$

By an induction on n, we conclude from (18) the following:

$$\boxed{\Phi_n(x) \text{ is a monic polynomial with integer coefficients and constant term } \pm 1} \tag{19}$$

For use in the next section, we rewrite (17) one more time. Suppose that k is a proper factor of n. Then, on the one hand, $x^k - 1$ divides $x^n - 1$ (see (10). And, on the other, we may partition the factors e of n into two sets: those that divide k and those that do not. We thus get:

$$x^n - 1 = \prod_{e|n} \Phi_e(x) = \left(\prod_{e|k} \Phi_e(x) \right) \Phi_n(x) \prod_{e|n, e \nmid k, e \neq n} \Phi_e(x) \tag{20}$$

The first of the three factors in the right hand side of the above is $x^k - 1$ by (17), and so we get:

$$\boxed{\frac{x^n - 1}{x^k - 1} = \Phi_n(x) \cdot \prod_{e|n, e \nmid k, e \neq n} \Phi_e(x)} \tag{21}$$

4.5. **Conclusions.** Suppose x is an integer. Then, from (19) it follows that $\Phi_n(x)$ is an integer; from (17) that $\Phi_n(x)$ divides $x^n - 1$; from (21) that $\Phi_n(x)$ divides the integer $(x^n - 1)/(x^k - 1)$ for k a proper factor of n.

5. The proof proper

We are finally ready to prove Wedderburn's theorem that every finite division ring is a field. We proceed by contradiction. Suppose that D is a finite division ring that is not a field. We fix notation as in §3. There exists a non-singleton conjugacy class in the group $D^\times$, which means that $n \geq 2$ and $\ell \geq 1$ in the class equation (9).

Consider the conclusions in §4.5 (with q being substituted for x). We see first of all that $\Phi_n(q)$ is an integer. Next we consider the divisibility by this integer of each of the terms in (9). From the second and third conclusions in §4.5, we see that $\Phi_n(q)$ divides $q^n - 1$ and in fact each of the terms $(q^n - 1)/(q^{k_1} - 1), \ldots, (q^n - 1)/(q^{k_\ell} - 1)$. Thus $\Phi_n(q)$ must also divide the only remaining term in (9), namely $q - 1$.

This means in particular that $|\Phi_n(q)| \leq |q - 1|$. But, as we show below, $|\Phi_n(q)| > |q - 1|$, which leads to a contradiction, and the proof is finished.

5.1. **Proof that $|\Phi_n(q)| > |q-1|$.** From the definition (16) of $\Phi_n(x)$, we see that $|\Phi_n(q)| = \prod_{k\in[n]_1} |q - e^{2\pi ik/n}|$. Since $n \geq 2$, we have $k < n$ for $k \in [n]_1$, so that $e^{2\pi ik/n} \neq 1$. We claim the following:

$$|q - e^{2\pi ik/n}| > |q-1| \text{ for each } 1 \leq k < n \tag{22}$$

Assuming the claim, we see immediately that $|\Phi_n(q)| > |q-1|^{\phi(n)}$. Since $\phi(n) \geq 1$ and $|q-1| \geq 1$ (since $q \geq 2$), we conclude that $|\Phi_n(q)| > |q-1|$.

As to the claim (22), it is obvious pictorially: since q is an integer ≥ 2, it is clear that the unique point in the unit circle on the complex plane closest to q is 1.

Here is an analytic proof, at any rate: Put $e^{2\pi ik/n} = a + b\sqrt{-1}$ (where a and b are real with $a < 1$). We have

$$\begin{aligned} |q - (a+b\sqrt{-1})|^2 = (q-a)^2 + b^2 &= q^2 - 2aq + a^2 + b^2 \\ &= q^2 - 2aq + 1 \qquad \text{since } a^2+b^2 = 1 \\ &> q^2 - 2q + 1 \qquad \text{since } a < 1 \\ &= |q-1|^2 \end{aligned}$$

and the claim (22) is proved.

THE INSTITUTE OF MATHEMATICAL SCIENCES, CHENNAI
E-mail address: knr@imsc.res.in